USCENTCOM Information Superiority Strategy For the New Millennium

December 1997

The quest for information superiority is a time honored military objective. Today our ability to routinely achieve this capability is within reach. In fact, the attainment of information superiority is absolutely key to the new operational concepts of dominant maneuver, precision engagement, focused logistics, and full-dimensional protection so clearly articulated in Joint Vision 2010. But, how do we begin?

We will start with this information superiority strategy. It will guide our efforts into the new millennium. We will apply it to our planning, exercises, and operations. This strategy will ensure we all work in concert to harness the full operational potential our Nation's advanced technology allows.

When first undertaken, such a quest can be daunting. This strategy will provide the guidance each of you needs to consistently bring your rich background of military experience into play. Properly embraced, this information superiority strategy is so designed that it will take us rapidly from the initial learning stage to an advanced capability.

I challenge each of you to internalize this strategy and to apply it appropriately to your individual areas of responsibility. Our success as a command hinges on our collective ability to master the consistent achievement of information superiority and to apply it successfully to the operational missions we face.

A. C. Zinni
General, USMC
Commander in Chief

TABLE OF CONTENTS

"A journey of a thousand miles begins with a single step." Ancient Chinese Proverb

USCENTCOM Information Superiority Strategy for the New Millennium

Synopsis:

The USCENTCOM information superiority strategy for the new millennium is designed to apply command-wide and is both current and long range. Information superiority is the enabler for the new operational concepts of dominant maneuver, precision engagement, focused logistics, and full-dimensional protection. To harness its fullest potential we must use the foundation and framework provided by this information superiority strategy to guide our individual and collective efforts over the long term.

There is a threat. It is real and growing. Today, hackers, disgruntled employees, and incompetence are a very real weakness. In the all-to-near future, the threat will expand to include terrorist groups, political dissidents, organized crime, and foreign espionage. To counter the threat, our achievement of information superiority must be grounded in a solid defensive posture and be an integrated command-wide effort. There is no one shot solution - - no silver bullet or magic BB.

The desire to achieve information superiority is as old as military conflict itself. What has changed is the medium and speed by which we do business. Like any new capability it has both strengths and weaknesses. Solutions for making information superiority work in our favor need to be based on sound military operational experience and the full appreciation of the opportunity costs of failing to act or acting in a half-hearted manner.

Offensive and defensive information operations are inter-related. One cannot be fully considered without the other. It helps to remember we are defending against someone else's offensive information operations.

To guide our actions, a vision, mission statement, and supporting goals have been developed. These are given further definition to guide our implementation by the doctrinal principles, planning considerations, and architectural tenets of the information superiority strategy.

Several operational terms - - critical intelligence, essential elements of information, and a basic load of information - - are addressed in this document. These terms are both familiar and also part of the educational effort needed to get us all actively thinking about our defensive posture. Finally, so we may provide coordinated emphasis through all means of influence available, the tools available to the Command are also discussed.

"We owe the men and women who may be in harm's way every edge technology can provide. Technology will never be a substitute for courage and human toughness in conflict, but it can increase the likelihood that the tough and courageous will be successful." Admiral William A. Owens, Vice Chairman, Joint Chiefs of Staff

Setting the Stage:

Arguably, the United States is the largest user of information technology in the world today. Our ability to bring technology to bear in conducting daily commercial and public business is a great strength. Indeed, our ever-increasing national capability has given rise to the concept of information superiority as the focusing lens of military power.

As we all know, the concept of information superiority is not new. In fact, a basic ambush is made possible by capitalizing on the simple use of information superiority. In the successful ambush, you know where the enemy is and he does not know where you are. This allows you to bring the principles of war to bear in your overwhelming favor. As they say in the infantry, no one walks away from a successful ambush.

What is new today is the concept of being able to routinely rely on the advantages flowing from information superiority. That means being able to routinely control what the enemy knows and being able to count on taking decided military advantage of our own superior information. In its most rudimentary forms, we have even been able to demonstrate that we can attain increased routine information superiority and can bring it to bear in military operations.

However, the coincident aspect of deriving great strength from the use of information technology is that it is also potentially our greatest weakness. It may even be our Achilles' heel. Some people go so far as to relate our over reliance on information superiority as a pending crisis.

As a military and as a command, our best outlook toward the concept of achieving routine information superiority may lie in the written Chinese word for crisis. The word consists of two characters. One character represents danger and the other represents opportunity.

The understanding of our seeking to use information technology to achieve routine superiority as a two edged sword will go a long way towards helping us keep an appropriate balance in our actions. Indeed there is danger, but failing to use technology to our advantage is not the answer. In fact, surrendering the initiative represents the greatest danger of all.

Seizing opportunity is something we in the military know how to do. Yet, even the most courageous may hesitate in the face of a threat that is so elusive as information dominance. Knowing the power of what can potentially happen on the offensive side - - and some of us may even have witnessed convincing demonstrations or been the victim of sophisticated hacker tools - - may only heighten our concern for the defensive side. Just because nothing has happened, how do we know for sure that our weapon systems and information are safe?

As a nation and as a military, we are even having trouble coming to grips with something as seemingly straight forward as the pending year 2000 problem. If we cannot rely on the computer to know that the year 1999 is followed by the new millennium, how will we be able to protect our information against the myriad of viruses, hackers, trap doors, Trojan Horses, and all sorts of other ethereal phenomenon? For many, this seems to be a true conundrum.

In the face of this seemingly overwhelming obstacle, it is useful to step back and look at the challenge from a base we are all comfortable with. Our experience and understanding of what we need to do will serve us well when provided with a few guidelines to point the way. Indeed, some of these guidelines are very basic.

The Iraqi bayonet and a piece of polished marble brought back as souvenirs from Operation PROVIDE COMFORT, the humanitarian effort to save the Kurds in southeastern Turkey and northern Iraq, serve to highlight the basic nature of the fundamentals of achieving successful information superiority. The liberated bayonet from Zakhu serves to remind us that in the midst of all the technology - - the fancy hardware and geewiz software - - we must remember the very basics of our profession.

Similarly, the polished marble from the airport that was being built in Sirsenk, Iraq - - to provide easy access to the summer palaces - - serves as a reminder that there are indeed very real opportunity costs in the world today. It seems quite fitting that both the bayonet and the marble were liberated from Saddam Hussein, an individual who neither understood the basics of our profession, or the opportunity costs of military adventurism.

"Four things come not back: the spoken word; the sped arrow; time past; the neglected opportunity." Omar Ibn

The Strategy:

In addressing the issue, the USCENTCOM information superiority strategy for the new millennium must be thought of as command-wide. It must be an integrated command-wide strategy that remembers the basics of our military profession as well as the opportunity costs associated with this aspect of warfare.

The strategy is also both current and long range. While the new millennium seems to still be a couple years in the future, we must remember that for several years now considerations for the year 2000 have been included in our budgeting process. In fact, this year the base line for the budget is the starting year for the new millennium. In the long-range view, this is not a passing fad. Information operations will be with us well into the next century. Indeed, well into the foreseeable future.

This paper has drawn heavily on current works, such as the November 1996 report by the Defense Science Board Task Force on Information Warfare - - Defense (IW-D). While the report itself is a year old, the Chairman's opening letter makes a most pointed reminder in stating, "this is the third consecutive year a DSB Summer Study or Task Force has made similar recommendations . . ."

The USSOCOM C4I Strategy has also been used as a source. Many of the information operations considerations being looked at today - - and by many of us for the first time - - have long been fundamental considerations for the successful conduct of unconventional warfare and special reconnaissance operations. The lessons learned since World War II by the Office of Strategic Services (OSS) and by today's Special Forces - - such as the need to encrypt traffic, the need for compartmentalization, and "the need to know" - - are basic to successful information operations and are readily available for those who choose to learn from previous experience. Yet, for those who ignore these fundamental considerations there is also a very real and potentially very large opportunity cost.

The USCENTCOM information superiority strategy provides both a doctrinal foundation and an architectural framework for accomplishing effective integrated command-wide information operations. There are a lot of neat capabilities and interesting toys available on the market today. A doctrinal foundation and architectural framework help us all by providing a common perspective. It also keeps us from becoming stockholders in the proverbial toy store of solutions looking for a problem.

- **Information Superiority:** "The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." Joint Vision 2010 and Joint Pub 3-13.

Information superiority by definition must be an integrated and command-wide effort. In trying to fully understand the concepts associated with information superiority, it helps to think of information in terms of data flow. Your voice, imagery, e-mail, facsimile, video teleconference or VTC, and so on, are all data. Some of today's systems and the new technology that will be commonplace by the year 2000 will treat all communications as standard cells of data. Used correctly, this trend will enhance our ability to attain and maintain information superiority.

The ability to control the flow of information - - to focus the proverbial lens of information superiority - - is the enabler for the new operational concepts of dominant maneuver, precision engagement, focused logistics, and full-dimensional protection. Achieving the desired sharpness of focus requires a continued command-wide effort across the full spectrum of conflict. That means that information superiority is neither a war time effort, nor a peacetime effort. Successful information operations are a full time effort.

The USCENTCOM information superiority strategy also draws heavily on Joint Vision 2010 and USCENTCOM's Strategic Plan. It provides a common command-wide basis for achieving effective and coordinated efforts both today and in the future.

In searching for solutions to this seemingly illusive concept called information superiority, we must remember our military experience is a valuable guide for working through the challenge - - there is no single solution. True effectiveness is achieved and maintained by continual effort over the long term. To that end, our efforts must focus on achieving a continuously improving operational capability.

"Make it a point to keep on the lookout for novel and interesting ideas that others have used successfully. Your idea has to be original only in its adaptation to the problem you are currently working on." Thomas Edison

The Vision:

- **Lead the evolution of information superiority into the new millennium, serving as the guardian of excellence and the engine of change.**

To properly look at information superiority on a command-wide basis, we first start with a vision to provide essential guidance over the long term. The three key aspects of this vision are:

- It is an evolutionary process.
- It must be done to a standard.
- It does require change.

The fast pace of technology says, in practical terms, that we must set ourselves up to evolve forward in knowledge and capability. This is not a one-time shot. It is a continuing challenge that calls for leadership well founded in the basics of our profession and ever mindful of the opportunity costs involved.

One of the essential basics is to be able to perform tasks, under stated conditions, and to a standard. As the guardians of excellence, we must ensure a level of offensive and defensive capability consistent with our needs as a command. For many of these tasks, there is no right or wrong answer, nor is there necessarily an answer that will be consistently correct from operation to operation. Rapidly developing technology and techniques - - both offensive and defensive - - require a periodic re-evaluation of the strengths and weaknesses of systems and networks followed by a conscious operationally based decision concerning their employment and use.

Change makes many people uncomfortable. Yet, to lead this evolution we must condition ourselves to continual change. Indeed, we must condition ourselves to be the creator of change. In the midst of this seemingly sea of change, there is one constant. The conditions under which we must perform the task to a given standard will always be, "during daily garrison and deployed operations" (see Appendix B). Successful information operations are a full time effort and require our full time attention.

"Successful companies of the 21st century will be those who do the best job of capturing, storing, and leveraging what their employees know."
Lewis E. Platt, Chairman, President and CEO, Hewlett-Packard

The Mission:

- **Be a catalyst to promote and implement the vision which ensures the command's capability to achieve information superiority continuously improves.**

- **Provide and sustain an information superiority capability for USCENTCOM forces to allow them to successfully operate in peace, operations other than war, and war.**

From our high school chemistry, we remember that a catalyst precipitates a reaction, but is not consumed by the process. This effort to achieve and maintain information superiority must not become an all-consuming raging fire. Rather, it must become an integral part of everything we do. We must routinely seek to improve our capability.

The reason for the never-ending push to continually improve is evident when we say, in the second part of the mission statement, that we must not only provide the capability, but also sustain it. This is a very real challenge given the explosive rate of change in technology.

The Goals:

- **Serve as the information superiority entrepreneur for USCENTCOM - - and beyond.**

- **Improve information superiority support to customers with systems based on our doctrine and architectural tenets.**

The information superiority goals present another new area that many people are not comfortable with - - success requires an entrepreneurial spirit. We must be the creators of initiatives that will apply command-wide and also outside the command. Achieving information superiority requires us to work both within the command and also beyond the command. The action - - or inaction - - of other commands has a direct bearing on USCENTCOM's information superiority capability.

Time and distance do not necessarily provide protection. We need only remember that during a recent military exercise, access to one Unified Command was achieved through a terminal in another Unified Command that was many time zones and thousands of miles away. Information superiority requires constant vigilance.

"We are confronted with insurmountable opportunities." Walt Kelly, "Pogo"

Information Superiority Principles:

- **Global**
- **Secure**
- **Mission Tailored**
- **Value Added**
- **Joint**

There are certain fundamentals in the profession of arms that everyone must know and understand. The principles of war - - objective, offensive, mass, unity of command, maneuver, economy of force, security, surprise, and simplicity - - together form such a fundamental. As we are taught in our schools, as we experience during exercises, and as we learn in our collective operational experience, the principles of war are just as valid today as they were in the past. Preserving the principles of war is fundamental to successful military operations.

Likewise, the information superiority principles are fundamental to success in the information age. These principles compliment and enhance our ability to achieve the principles of war on the battlefield. As part of our on-going effort to stay current in the profession of arms, the information superiority principles must now be added to our kit bag of tools.

- **Global:**

  The principle of global applies directly to the U.S. Central Command. We do not live in our area of responsibility (AOR). Therefore, for even the most routine operations, we are extremely reliant on a great deal of information flow between the CONUS and our AOR, some 7,000 miles away.

  Our requirements also draw on worldwide support from national level resources. Supporting CINCs, the Services, and agencies provide intelligence, logistics, telemedicine assistance, personnel replacements, public affairs information, and so on, that this command must have to function.

  Indeed, the success of our operations depends on global interaction. Quite literally, we are all in this together.

- **Secure:**

  By secure, we mean National Security Agency (NSA) provided codes and ciphers. NSA provided security is the best protection we can provide to our people and to our operations. It is not always easy to protect our data flow, but it is something we must continually strive to do.

  Additionally, maximum use must be made of classified systems, such as, secure voice and the Global Command and Control System (GCCS). These systems protect the data flow from end-to-end and ensure the integrity of our transmissions.

While there may also be systems we rely upon that are not encrypted, we need to proactively work to get them protected. In the interim, we need to follow the basics that have applied to radio transmissions for years. All traffic, classified and unclassified, must be - - as a minimum - - bulk encrypted for transmission.

- **Mission Tailored:**

  Successful information superiority is achieved by tailoring to the mission and task organizing to support the customer and the operation. This means we must look at how our component units are organized and equipped. Organizations and equipment designed for World War III in Europe are not necessarily optimized for war in the information age.

- **Value Added:**

  Many advantages are achieved by leveraging rapidly advancing technology. However, we must always ask ourselves up front, "What are the risks and disadvantages of this capability?" Our challenge is to ensure the technology we choose is value added to our forces.

  Certainly everyone would agree, by the use of our technology we must never compromise a unit, a team, or an individual operator. And yet, we have.

  Two examples serve to illustrate the point. During Operation Desert Storm, we lost pilots to the Iraqis due to a weakness in our information operations posture. The pilots were equipped with a PRC-90 survival radio that broadcast on two separate international distress frequencies. After the pilots were shot down, as instructed, they turned the radios on and it became a time-distance contest favoring the enemy.

  We also lost special operations forces trying to rescue the downed pilots. This was not value added to either the special operations forces or to the pilots. It would have been better if the pilots had not turned the radios on than to fire the proverbial red star cluster that told the Iraqis exactly where they were.

  The second example occurred during Operation Desert Shield when the Iraqis attacked Khafji. As the out numbered U.S. forces pulled back rapidly, a rucksack was left behind containing everything the individual owned, to include a radio and three months of the cryptographic key. The matter was made worse by the fact that the three months worth of key lost was also part of the Inter-Theater COMSEC Program (ICP). It was the key being used by the entire theater of operation. Again, by not acting well in advance of the event to plan for alternative keying material after units arrived in theater, we allowed our forces to be put in an unfavorable position.

- **Joint:**

  As the previous discussion and examples illustrate, the Air Force or Navy pilots may be rescued by another Service or all forces may be affected by a cryptographic compromise. Information superiority operations are inherently joint.

Planning Considerations:

- **Information superiority largely depends upon National systems.**
- **Information superiority must be provided down to the lowest possible tactical level.**
- **Communications systems do not follow the chain-of-command.**

We have a vested interest in National systems for intelligence, logistics, communications, command and control, and information superiority. Our planning must recognize the strengths and weaknesses of our reliance on these systems.

While the specific information needs may differ, the principles of war and the principles of information superiority apply to all levels of operation. Even the foot soldier is dependent on the Global Positioning System (GPS) for navigation.

Today's - - and tomorrow's - - distributed network information systems are a fact of life and are also different than many of us are used to. We must educate ourselves to make wise use of their increased potential while simultaneously minimizing their weaknesses.

"We know what we are, but know not what we may be."   William Shakespeare

Architectural Tenets:

- **Seamless**
- **Robust**
- **Automated**
- **Full Spectrum**
- **Standards Compliant**

The architectural tenets compliment the information superiority principles and position us to make wise use of the increased potential of our networked systems.

- **Seamless:**

  The tenet of seamless says we must allow information to flow freely through networks as operationally required. This seamless flow of data addresses the element of time. Much of the data flow is of direct use to forces without the intervention of intermediate headquarters. The need for information flow is not the same as the chain-of-command. Rather, it is a function of carrying out the desires of the chain-of-command so information superiority is gained and maintained.

- **Robust**

  By robust, we mean to provide multiple means of communication to support our operations. As reliant as we are on the free flow of data, we must make sure our forces - - and we - - are never single point sensitive. We must ensure we can never be isolated by a single failure.

  An integral part of seeking the affordable robustness we need is to harness the power of switched systems to provide many alternative routes for communications to flow. Properly engineered, modern switched networks do automatic alternate routing around points of congestion and failure. In many ways, they are self-healing.

  One of our greatest challenges is to provide a communications architecture that is flexible and adaptable to the changing needs of the command. While we cannot get there overnight, we must ensure a command-wide emphasis is maintained towards rapidly achieving this tenet. This command-wide attention will, by necessity, mean using the tools discussed later to influence other commands and agencies to change the way they currently do business. In large measure, our ability to ensure information superiority depends on it.

- **Automated:**

  This tenet builds on the two before it. Many of the necessary functions in information operations are most effective or only effective when they are automated. The tenet of automated says we need to harness automation for what it can do best and to free the operators to do what they can do best.

- **Full Spectrum:**

  The frequency spectrum is a precious resource that must be carefully allocated and proactively managed. It is through the use of the frequency spectrum that the communication systems carrying the required data flow are made to work. When the frequency allocation fills up, we become physically limited in how much data flow we can handle. However, if we can use other portions of the frequency spectrum then we can often simply switch to an available portion and continue to do business. Our emphasis needs to be to increasingly attempt to utilize the full frequency spectrum.

- **Standards Compliant:**

  Our operational support is enhanced by being standards compliant. While under the banner of interoperability we have long sought standards compatibility among the Services, the information age and the need for information superiority require different priorities. In fact, at first blush the priorities appear to be just the reverse from what we would expect.

  To harness the power of the distributed networks and switched systems and to take full advantage of the vast worldwide global network of commercial systems we seek compliance in the following order. We seek first to use international commercial standards, then U.S. commercial standards, and then finally, if and only if there is an overriding operational reason or no other standards exist, to use military standards.

Like the principles of war they compliment and enhance, the doctrinal principles and architectural tenets described are easily understood on the surface, but have tremendous ramifications on the actions we take. A story from a management class, that is reported to be from a major aircraft manufacturer, may help put these new principles and tenets in perspective.

According to the story, whenever an engineer had a hot idea for the President, such as the concept for a new aircraft, it was frequently quite complex. The President's solution was to offer a business card to the engineer and to ask the engineer to put the essence of his idea on the back of the card. Inevitably, the response would be that his ideas for the new aircraft were far too complex to fit on the back of a business card. The President's reply to the engineer would be, "Then the idea is not ready for me yet."

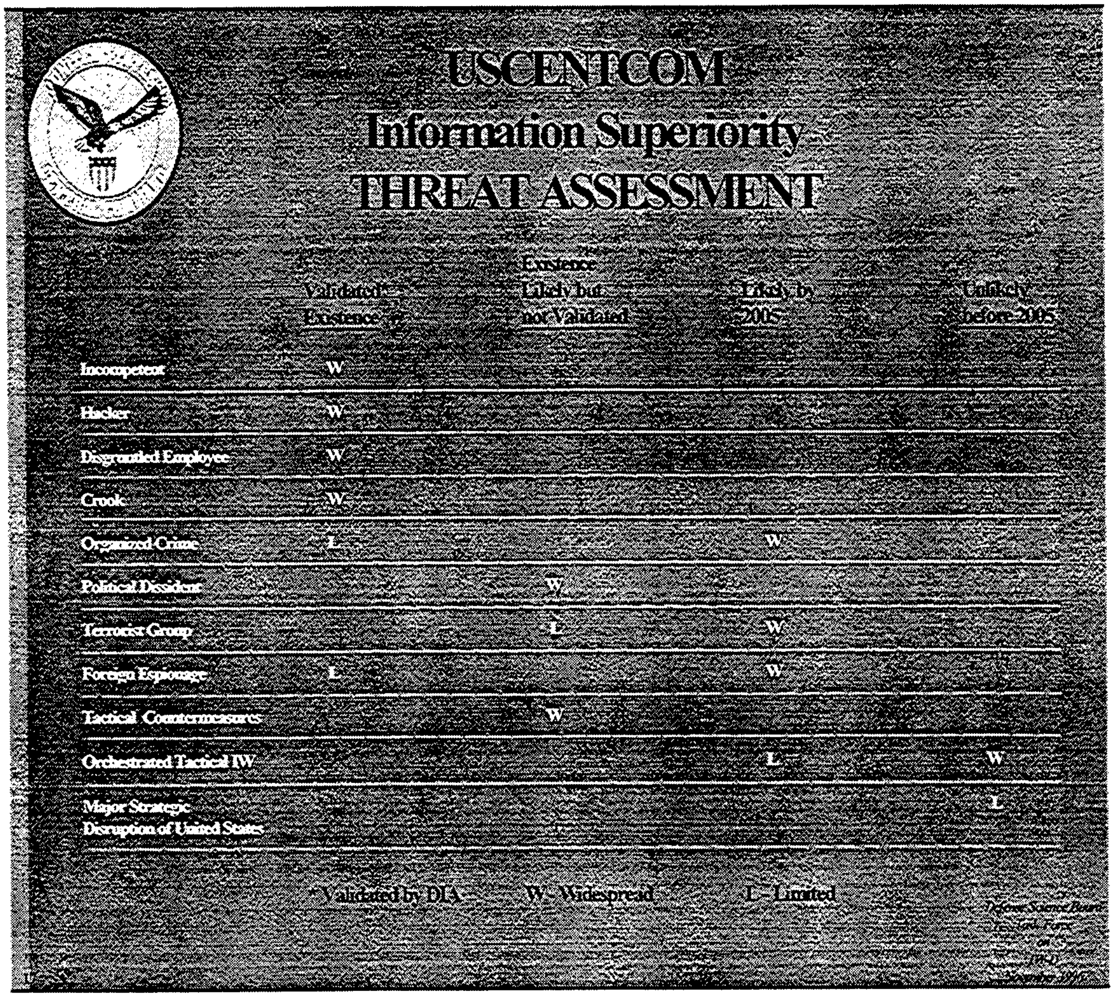
In all likelihood, more than one person reading this paper will say to themselves that the engineer was correct. The ideas behind an aircraft as complex as a modern airliner simply would not fit on the back of a business card. Yet, when properly thought through, the essence of such complexity can indeed fit neatly in a small space. For example, the ideas and the thought process behind the equation E=mc2 are very complex, but fit neatly on a business card. Likewise, the thought process behind the doctrinal principles and architectural tenets of information superiority is complex. Yet, these principles and tenets also fit neatly on the back of a business card.

“A new idea is first condemned as ridiculous, and then dismissed as trivial, until finally it becomes what everybody knows.” William James

Defensive Information Operations (DIO):

To properly address information superiority, we must understand that the offensive and defensive operations are interrelated. One cannot be fully considered without the other.

In developing this paper, the threat assessment was taken from the Defense Science Board Task Force on IW-D, dated November 1996. It says quite clearly that the threat is out there. The threat is here today and will continue to grow into the new millennium. By the year 2005, we expect widespread use by organized crime, terrorist group actions, and foreign espionage. While the rest of this paper will concentrate on defensive information operations (DIO), the key is that we are defending against someone else's offensive information operations.



USCENTCOM
Information Superiority
THREAT ASSESSMENT

	Validated* Existence	Existence Likely but not Validated	Likely by 2005	Unlikely before 2005
Incompetent	W			
Hacker	W			
Disgruntled Employee	W			
Crook	W			
Organized Crime	L		W	
Political Dissident		W		
Terrorist Group		L	W	
Foreign Espionage	L		W	
Tactical Countermeasures		W		
Orchestrated Tactical IW			L	W
Major Strategic Disruption of United States				L

*Validated by DIA W - Widespread L - Limited

Defense Science Board Task Force on IW-D November 1996

Figure 1: Threat Assessment

The first rule of defense is to know yourself - - your strengths and your weaknesses. The rapid advances in technology, the increasingly inter-related nature of global communications, business, and information systems, as well as, the leading role the United States plays in world affairs, all add up to the fact that the quest for successful defensive information operations has no finish line. DIO must be an integral part of everything we do.

If there is a bottom line to defensive information operations, it is continuing education and training. While a single lapse in our defensive posture can make us vulnerable to an attack, keeping all the holes plugged from a defensive point of view requires constant effort and monetary investment. There are no easy solutions. Effectiveness is achieved and maintained by continual effort over the long term. As stated earlier, our efforts must focus on achieving a continuously improving operational capability.

"Nothing is worse than active ignorance." Johann Wolfgang Von Goethe

Defensive Information Operations: An Instrument of Combat Power.

The pervasiveness of the considerations needed to achieve and maintain information superiority says we need to view it in a similar way to the other instruments of combat power.

- **Critical Intelligence:** "Intelligence which is critical and requires the immediate attention of the commander. It is required to enable the commander to make decisions that will provide a timely and appropriate response to actions by the potential/actual enemy . . ." Joint Pub 1-02.

- **Essential Elements of Information (EEI):** "The critical items of information regarding the enemy and the environment needed by the commander by a particular time to relate with other available information and intelligence in order to assist in reaching a logical decision." Joint Pub 1-02.

On a daily basis, in CONUS, in our AOR, and for a specific country or operation, there are certain elements of information important enough to wake the commander up, even if he has just gone to sleep after a prolonged period without rest. These elements would indeed be critical intelligence. Other information is essential to decision making and needs to be kept current and visible to the commander and staff alike. These elements are essential elements of information. From the point of view of information superiority, an example of both critical intelligence and essential elements of information might be presented as follows:

Critical Intelligence:

- Basic load of information: specific country or operation.

Essential Elements of Information:

- Basic load of information: CONUS, AOR.
- National systems' status: generic capabilities; e.g., secure voice (Red Phone, STU III, Grey Phone, STO Phone).
- Command systems' status: CONUS, AOR, specific country or operation.

Based on the doctrinal principles and architectural tenets of information superiority, we need to watch the National systems' status and the command systems' status. These views keep the commander informed on the relative ability of the various communications systems (including intelligence systems) to allow data flow. It also helps to prioritize restoration efforts.

The basic load of information - - shown above as an example - - is split between the essential level for CONUS and our AOR and the critical level for a specific country or operation. The concept of a basic load of information is new and requires amplification.

Rules for a Basic Load of Information:

- **Have a minimum of 72 hours of data information required to do your job.**
- **Have, as a minimum, enough historical data to do your job for 90 days.**
- **Carry with you all the non-changing data required to do your job.**

Just as a weapons system - - an individual soldier, tank, aircraft, or ship - - would have a basic load of ammunition and supplies, they must also have an appropriate basic load of information. For the individual Marine or infantryman, the basic load of information may be as simple as the commander's intent, the five-paragraph field order, a map, and a compass azimuth. That basic load of information may also provide enough knowledge for mission accomplishment for 12, 24, 48, or even 72 hours.

At higher levels, the situation gets more complex. However, we still need to continually seek the answers to, "What is my basic load of information?" and "How long will that basic load of information last?" The answers to these questions not only help us prioritize restoration efforts during the immediacy of a current operation, but also over the long term allow us to work to reduce vulnerabilities..

"I look for what needs to be done . . . that's how the universe designs itself."
R. Buckminster Fuller

The Tools to Do the Job:

As a direct result of our dependence on the global flow of data, we must use all of the means of influence at our disposal to ensure a solid defensive posture. There are a variety of tools to chose from and, in many cases, multiple tools will need to be used to attain the desired result. The following is a partial list:

- National Military Strategy
- CINC's Integrated Priority List (IPL)
- Joint Warrior Capability Assessment (JWCA)/Joint Requirements Oversight Council (JROC) Process
- Joint Military Readiness Report (JMRR)
- Budget
- CINC's Strategy
- Policies, Procedures, and SOPs for HQs, Components, and Individual Directorates
- OPORDS/OPLANS
- Joint Doctrine
- Tasking, e.g., the Defense Information Systems Agency (DISA) and the National Security Agency (NSA)
- Training
- Education
- Writing for Publication

The list purposely includes writing for publication so those we wish to influence - - both within the command and beyond - - are given the benefit of the logic behind what we are doing and can also become educated in defensive information operations.

Through education, by the coordinated use of the many tools at our disposal, and through a unity of effort, we can achieve and maintain a continually improving operational capability in defensive information operations.

"Minds are like parachutes, they only function when they are open."
Sir James Dewar

Summary:

Achieving and maintaining information superiority is similar to the situation depicted in the African fable that says:

Every morning in Africa, a gazelle wakes up. It knows that it must run faster than the fastest lion or it will be killed!

Every morning in Africa, a lion wakes up. It knows that it must run faster than the slowest gazelle or it will starve to death!

It doesn't matter whether you are a lion or a gazelle - - when the sun comes up, you had better be running!

Indeed, attaining and maintaining information superiority is a race. It is a race we are already running. It is a race we must continually lead.

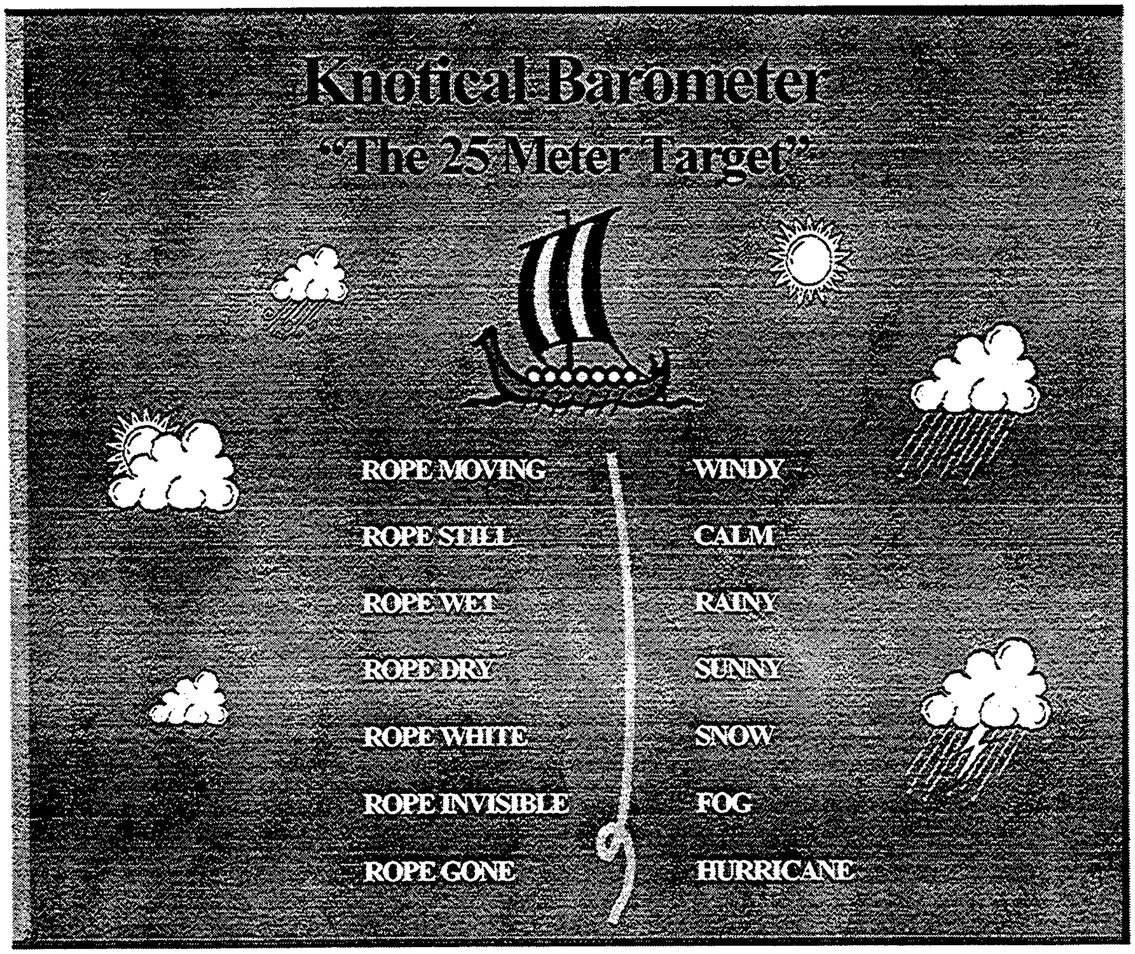
Success depends on a team effort. Each of us brings experience to the operation that others need. Each of us can also learn from what others are doing. Each of us will have to pass on to our replacement what we have learned. The information superiority marathon is unique in that the entry is open to anyone, teams can compete, and there is no finish line. In other words, we are at war.

"Even if you are on the right track, if you stand still you'll get run over by the next train." Will Rogers

APPENDIX A:

The 25-Meter Target: A Practical Example.

The USCENTCOM information superiority strategy for the new millennium provides guidance for the close in fight as well as the deep battle. However, since it is often difficult to look deep, see deep, and think about the deep battle while the close in targets keep popping up in profusion, an example of a 25 meter target may help provide clarification and perspective. In the interests of time and simplicity, this example will use the staff weather expert and consider the strategic to JTF levels of data flow. Just as will need to be done in each functional area, to fully complete the picture, the analysis would be finished down to the lowest tactical level by each directorate and component.



Knotical Barometer

"The 25 Meter Target"

ROPE MOVING	WINDY
ROPE STILL	CALM
ROPE WET	RAINY
ROPE DRY	SUNNY
ROPE WHITE	SNOW
ROPE INVISIBLE	FOG
ROPE GONE	HURRICANE

Figure 2: Everyone Predicts the Weather

The weather folks were chosen for two reasons. First, most people consider themselves to be knowledgeable of the weather and of what the weather people do. So we can easily relate to the example (see figure 2). Second, Xena - - the Air Force Weather Communications Vision - - closely follows this strategy. Xena uses the same doctrinal principles and architectural tenets outlined in the USCENTCOM information superiority strategy for the new millennium. Examining the doctrinal principles, planning considerations, and architectural tenets, as they relate to the way the actual weather support is provided today, may help the reader of this document to tie the undeniable presence of the 25-meter target with the longer-range strategy.

In simple terms, on a daily basis raw and model weather data is collected from two major CONUS sources, combined with local observations, reviewed in respect to historical data, and the appropriate forecasts prepared. Essentially, this same procedure is followed both in garrison and while deployed. Viewed in relation to the doctrinal principles, we find a majority of strengths as well as some weaknesses to work on.

Doctrinal Principles:

Global:

The Fleet Numerical Meteorological and Oceanography Center (FLENUMETOCCEN) in Monterey, California and the Air Force Global Weather Central (AFGWC) at Offutt AFB, Nebraska are the sources of raw and model simulation data used by our forces on a global basis. Local observations provided by the respective national governments are also important sources of data in preparing the daily forecasts. The Naval Oceanographic Office and the Air Force Climatology Center issue annual historical updates giving a preferred minimum of 10 years of data. Less than 10 years of historical data - - depending on the exact geographic location in the AOR - - is suspect. These sources are used in support of the full spectrum of conflict.

Analysis: big strength, slight weakness. The centralized capabilities are far more powerful than widely dispersed forecasters could produce on their own. However, the products must be distributed to be of value to the commander.

Secure:

One way to access the global sources of information is via the Secure Internet Protocol Router Network (SIPRNET). These global sources are open to anyone having access to the SECRET level network. Both the Global Command and Control System (GCCS) and "INTELink S" are National Security Agency (NSA) approved secret level networks that use the SIPRNET and allow access to both CONUS weather centers. The Non-classified Internet Protocol Router Network (NIPRNET) also provides access to the same information and is password protected, but provides no NSA encryption.

Commercial phones, with modems, also provide an unclassified dial in capability to CONUS weather facilities. Like its NIPRNET counterpart, this unclassified access is password protected. There is no STU III dial in capability.

Analysis: strengths and weaknesses. NSA secure networks provide the single best protection we can provide our forces. However, they are still vulnerable to the current threat of disgruntled employees, incompetent users, and internal hackers. Good defensive information operations would add password protection, such as exists for users who access the data through the NIPRNET. The password protection for both NIPRNET and commercial phone users also needs to incorporate the routine use of common hacker tools by the system administrators at the central depositories. This will ensure the passwords provide the best degree of protection possible.

A recent check of 1,300 users at a unified command found 300 easily broken passwords on the first check. This was the initial check run after conversion to a new operating system. After the first check, the users were notified to change their passwords following standard practices designed to guard against known hacker procedures. The second check found no passwords that could be broken.

The significant point is that, while the protection we seek is afforded by a series of protective measures, all firewalls are not equal. Nor do all passwords provide the same degree of protection. There is a difference in quality.

While passwords help protect against unauthorized users, they do not protect either the information request itself or the response. Weather requests about predicted winds aloft or about predicted sea states could easily provide a tip-off about an impending airborne or an amphibious operation. Unclassified requests for weather information in support of operations is a definite weakness.

Mission Tailored:

As military requirements develop, major CONUS centers serve as resources to forecasters worldwide. For example, in preparation for an airborne operation, the volumes of available data that are not needed - - such as tide tables and sea states - - is ignored while the required information - - such as light data and predicted winds aloft - - for the specific operational area is pulled. Similarly too, local observations and historical data can be tailored to support the desired end product.

Analysis: big strength. The common practice employed here is known as "user pull" and makes efficient use of the transmission media to support the required data flow.

Value Added:

The relatively easy access to the large volumes of warehoused raw data and the products of powerful simulation models provide accuracy and the ability to analyze variables that would otherwise not be available. Since only the data requested and the products of the simulation models are passed, efficient use is made of the transmission media. Most importantly, the deployed commander has access to tools not otherwise available.

Analysis: big strength. The value added is obvious and the one possible weakness - - that of an intruder being able to corrupt the data - - is greatly minimized by the computer models themselves as well as the "man-in-the-loop." It just so happens that the nature of the weather forecaster's business means that they frequently are provided bad data. Inaccurate readings or readings improperly entered and transmitted must be screened out by the individuals using the information. Due to the routine use of historical data, the forecaster usually knows the normal expected range of the readings.

Joint:

Weather operations draw heavily from joint doctrine. They also capitalize on the various Service areas of expertise to provide truly joint capabilities and products.

Analysis: big strength. The weather services are making maximum use of joint common user systems. To do so, they must be standards compliant. The end result is the effective use of data transmission resources and the ability to exercise maximum flexibility in the accomplishment of their mission.

Planning Considerations:

The weather capability also follows the information superiority planning considerations quite closely. The weather forecasters make maximum and wise use of the National systems and provide parallel capabilities down to the lowest possible tactical level. Likewise, their effective use of these systems recognizes the strength of distributed networks that do not follow the chain-of-command.

Architectural Tenets:

When the weather operations are reviewed in relation to the architectural tenets, we again find a majority of strengths as well as some weaknesses to work on.

Seamless:

The tenet of seamless is fundamental to the accomplishment of Xena, the Air Force Weather Communications Vision. It is key to their global support of their customers. By the very nature of the way they do business, they have accomplished this objective.

Analysis: big strength. The only caution here is that technology is evolving rapidly and there is a constant need to modernize. This translates to ensuring there is adequate money in the budget to upgrade equipment as the common user systems and the common user software evolve independently.

The Defense Information Systems Agency (DISA) is key for staying seamless on a global basis. The USCENTCOM/J6 is the primary source for internal standards. Working together, they can ensure the seamless tenet stays a big strength for the command.

Robust:

The routine use of multiple common user systems - - such as the SIPRNET, the NIPRNET, and the Global Broadcast System (GBS) - - local observations, and historical data provide a very robust capability. This tenet drives the way the weather business is assessed. As a result, the weather forecaster is well positioned to work through adversity.

Analysis: big strength. By being able to use all means available, weather enjoys an enviable position. Barring a major and prolonged attack on our communications infrastructure, they will be able to get the information they need. Even if cut off completely; local observations, historical data, and the ability to run micro-scale models will permit the production of acceptable forecasts.

Automated:

The weather business has automated extensively and yet maintained the "man-in-the-loop" to good advantage. The use of computers and easily transportable software and historical data using CD ROM technology, together with positioning skilled personnel with the commands they support, is the smart combination called for by this tenet. They have indeed harnessed automation for what it can do best and freed the operators to do what they do best.

Analysis: big strength.

Full Spectrum:

Due to the collective actions taken by the weather operations personnel, they make maximum use of the frequency spectrum available today - - and maybe even better use of HF than many other functional areas. They are also planning to use other portions of the frequency spectrum, such as offered by the Global Broadcast System (GBS), as soon as it is routinely available worldwide.

Analysis: big strength.

Standards Compliant:

In pursuit of this tenet, the weather personnel have gone as far as they can go alone. Further progress is the domain of DISA and the J6.

Analysis: big strength, significant weakness. The big strength is that at the present, for what can be done practically by the weather service organizations, they have achieved this tenet. The significant weakness is that until commercial standards are set and in place, this Command can not fully capitalize on the seamless robustness provided by the rapidly evolving international commercial service providers. Today, the international standards for the Asynchronous Transfer Mode (ATM) are forecast to be in place by late 1999. Yet, DOD does not yet have a policy in place requiring conversion to ATM by the year 2000. Since the budget for the fiscal year 2000 has been completed, that means we may not have money in-place to make the conversion, nor be able to truly capitalize on the robustness of international commercial networks.

A number of the Command's tools can be brought to bear on this weakness. The near term, and most readily accomplished, is the JWCA/JROC process. The readiness report (JMRR) is another effective tool. Once the needed policy is in place and the ATM conversion is programmed, the CINC's Integrated Priority List (IPL) will help keep the issue in the spotlight. Other tools - - such as writing for publication - - can also help educate people to the importance of the issue.

One caution is in order. This is a quick look at a single staff function. The weather function is likely one of the most healthy in terms of defensive information operations. In all probability, a review of the remaining staff functions will not only further support this analysis, but also provide other areas of weakness as well.

Basic Load of Information:

Finally, we turn to the basic load of information for the weather personnel both at home and in the AOR. Again, from the information superiority perspective, the weather staff is well prepared. Information superiority is neither a wartime effort, nor a peacetime effort. Successful information operations are a full-time effort and the weather staff uses essentially the same tools, sources, historical information, and common user networks in garrison and when deployed.

Rules for a Basic Load of Information:

- **Have a minimum of 72 hours of data information required to do your job.**
- **Have, as a minimum, enough historical data to do your job for 90 days.**
- **Carry with you all the non-changing data required to do your job.**

The basic load of information for the USCENTCOM JTF stand-alone weather capability allows a variety of equipment to be used effectively. This equipment includes:

- A small tactical terminal (STT) which is a satellite receiver capable of direct feed from satellites overhead. It is also Internet Protocol (IP) network capable which facilitates the seamless exchange of data.

- Three desktop or laptop computers for accessing CONUS weather facilities via SIPRNET or NIPRNET. Weather data obtained varies from raw data, to model output, to large scale "man-in-the-loop" finished product.

- A tactical forecast station (UNIX) to access the grided database via the SIPRNET and the NIPRNET.

- Navy tactical environmental support system (TESS) to access oceanographic data via the SIPRNET and the NIPRNET.

- Commercial phones, with modems, to provide an unclassified dial in capability to CONUS weather facilities. Weather data obtained is the same as through the computer, but much slower.

- The charts and maps used by weather personnel are provided as part of the product from both CONUS based sources and via the satellite. Other charts and maps are produced locally from the data on hand.

SOPs and deployment binders contain historical data and written regional climatological studies by experts.

The basic load of information is updated constantly and is good for 2 to10 days of operation without refreshment, depending on the situation - - METT-T (mission, enemy, terrain, troops, and time) plus seasonal and geographical considerations. However, a significant shortfall is that the basis of weather prediction relies on cooperation of all the world's governments. Regional stress can cause drastic change in the availability of host nation, coalition, and - - naturally - - enemy data. Over time, the quality of the data will degrade if local observations for individually perceived national security reasons are not made available.

"Know the ground, know the weather, your victory will then be total." Sun Tzu

APPENDIX B:

Note: The mission essential tasks in this appendix were originally written for USCENTCOM Exercise INTERNAL LOOK 98. However, these tasks are universal and should be routinely applied to operations and exercises. Their routine use will help provide some of the key metrics necessary to judge the progress of an organization in providing a continuously improving defensive information operations posture.

Defensive Information Operations (DIO) Mission Essential Tasks For Exercise INTERNAL LOOK 98

Exercise INTERNAL LOOK 98 provides an opportunity to take a command-wide look at defensive information operations (DIO) from a systems perspective. Most of the capabilities we rely upon were developed over the years to satisfy individual or limited network requirements. While these capabilities may satisfy operational needs, they may also make us vulnerable to offensive information operations. Following the guidelines of the Information Superiority Strategy, this review will document our strengths and our weaknesses. Once documented, we can better capitalize on our strengths and move quickly to minimize our weaknesses.

DIO mission essential tasks are keyed to the Information Superiority Strategy's doctrinal principles, planning considerations, and architectural tenets. The general category applies to everyone. Consistent with the information superiority strategy, individual components and directorates must develop the tasks, conditions, and standards of the specific category of mission essential tasks to fit their operational situation.

Note: For many of these tasks, there is no right or wrong answer, nor is there necessarily an answer that will be consistently correct from operation to operation. Rapidly developing technology and techniques - - both offensive and defensive - - require a periodic re-evaluation of the strengths and weaknesses of systems and networks followed by a conscious operationally based decision concerning their employment and use.

A. General:

1. Doctrinal Principles.

- **Global**:

Task: Apply the same DIO measures to all systems used by or supporting the Command.

Condition: During daily garrison and deployed operations.

Standard: Consistent DIO standards are applied throughout the Command to keep USCENTCOM above the point of vulnerability.

- **Secure**:

Task: Communications systems will be encrypted for transmission.

Condition: During daily garrison and deployed operations.

Standard: 100% of the communications systems used are - - as a minimum - - bulk encrypted.

Task: Utilize a secure means of communication as the primary way of conducting business.

Condition: During daily garrison and deployed operations.

Standard: 100% of business is conducted using secure communications means.

- **Mission Tailored**:

Task: Tailor access to information on a need-to-know basis.

Condition: During daily garrison and deployed operations.

Standard: Access to information is consciously granted on a need-to-know basis.

Task: Use compartmentalization with password protection on data systems, e.g., GCCS and "home pages."

Condition: During daily garrison and deployed operations.

Standard: Access to information is consciously granted on a need-to-know basis.

- **Value Added**:

Task: Evaluate systems to determine their "value added" components, i.e., strengths and weaknesses.

Condition: During daily garrison and deployed operations.

Standard: Considering our own offensive information operation capabilities, categorize the applicable properties and characteristics of the systems.

Task: Employ systems to capitalize on their "value added" strengths and to minimize their weaknesses below the point of vulnerability.

Condition: During daily garrison and deployed operations.

Standard: Employed systems have known strengths and weaknesses and are employed so they present an operationally acceptable risk.

Task: Properly handle advanced warning of information operation attacks, actual attacks, and attempts at penetration in accordance with standard operating procedures (SOP).

Condition: During daily garrison and deployed operations.

Standard: SOP are in place and everyone is trained to handle advanced warning of information attacks, actual attacks, and attempts at penetration.

- **Joint**:

Task: Communications systems present equal ease of access to the Headquarters and to the Components.

Condition: During daily garrison and deployed operations.

Standard: Electronic voice, data, and VTC systems are directly accessible by those with a need-to-know.

2. Planning Considerations.

- **Information superiority largely depends upon National systems.**

Task: Make maximum use of National systems.

Condition: During daily garrison and deployed operations.

Standard: Effective use is made of National systems in support of operations.

- **Information superiority must be provided down to the lowest possible tactical level.**

Task: Engineer systems to allow need-to-know accessibility from the lowest possible tactical level.

Condition: During daily garrison and deployed operations.

Standard: Conscious operational decisions are made in determining requirements for need-to-know accessibility down to the lowest tactical level.

- **Communications systems do not follow the chain-of-command.**

Task: Engineer systems to provide maximum effective information flow.

Condition: During daily garrison and deployed operations.

Standard: Systems are engineered to capitalize on their technical capabilities to provide maximum effective information flow, e.g., switched common-user networks.

3. Architectural Tenets.

- **Seamless**:

Task: Provide communication systems that allow the unimpeded flow of information throughout the Command on an "as required" basis.

Condition: During daily garrison and deployed operations.

Standard: Communications systems across the Command allow for the unimpeded flow of required information, i.e., full interoperability.

- **Robust**:

Task: No capability or organization is vulnerable to isolation by a single failure (single point sensitive).

Condition: During daily garrison and deployed operations.

Standard: A minimum of two separate means of communication is provided to prevent single point sensitivity of any capability or organization.

- **Automated**:

Task: Identify operations that can be improved by automation.

Condition: During daily garrison and deployed operations.

Standard: Routine and repetitious procedures are automated to the maximum extent possible.

Task: Identify automated operations that can be improved by using a manual process.

Condition: During daily garrison and deployed operations.

Standard: Automation is appropriately applied to the operation.

- **Full Spectrum**:

Task: Determine the portions of the frequency spectrum that can satisfy each operational requirement.

Condition: During daily garrison and deployed operations.

Standard: Each requirement must be capable of being satisfied by a minimum of two distinct portions of the frequency spectrum.

- **Standards Compliant**:

Task: Determine the standards for each capability and rank order by: international commercial standards, U.S. commercial standards, military standards, and no common standards (proprietary).

Condition: During daily garrison and deployed operations.

Standard: Standards should follow the priority order of international commercial standards first, then U.S. commercial standards (if there are no applicable international commercial standards), and finally - - if and only if there are over-riding operational requirements or no commercial standards - - use military standards.

B. Specific: To be published by individual staff directorates, sections, and operational elements.

C. Essential Elements of Information:

- Status of National systems: Green, yellow, or red in terms of being able to provide the required data flow for the deployed command to maintain information superiority.
- Status of Command systems: Green, yellow, or red in terms of being able to provide the required data flow for the deployed command to maintain information superiority.

D. Basic Load of Information:

Task: Determine a basic load of information for the individual staff directorate, section, or operational element.

Condition: During daily garrison and deployed operations.

Standard: The basic load of information must be sufficient to allow the unit to adequately accomplish its mission for 72 hours.

Task: Maintain a basic load of information throughout the operation (pre-deployment, deployment, operation, and recovery).

Condition: During daily garrison and deployed operations.

Standard: Each functional portion of staff and operating entity maintains enough information to adequately accomplish the mission and commander's intent for a 72-hour period.

24 October 1997

"Management by objective works if you first think through your objectives. Ninety percent of the time you haven't." Peter F. Drucker

"Nothing great was ever achieved without enthusiasm."

Ralph Waldo Emerson